(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000137649 A**

(43) Date of publication of application: **16.05.00**

(51) Int. Cl **G06F 12/14**
H04L 9/10

(21) Application number: **11292595**

(22) Date of filing: **14.10.99**

(30) Priority: **23.10.98 US 98 178529**

(71) Applicant: **XEROX CORP**

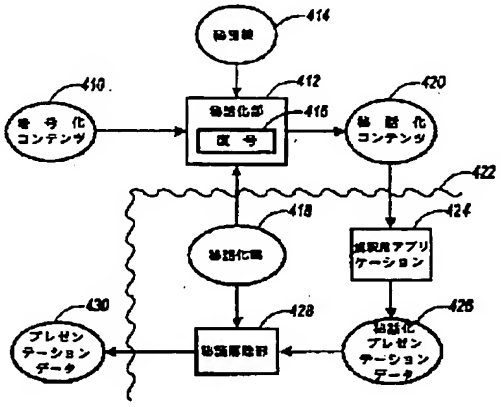
(72) Inventor: **PRASAD RAM**
TAN T TA
JIN WAN

(54) **SELF-PROTECTION DOCUMENT SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To obtain no electronic document in a redistribution-possible form at the time of a decoding processing and an interpretation processing by storing a self-protection document having data containing a ciphering content segment, a permission segment and a code segment.

SOLUTION: A self-protection document having a ciphering content segment, a permission segment and a code segment. In such a case, a document content 410 is transferred to a ciphering part 412. The ciphering part 142 receives the secret key 414 of a user and decodes the document content 410 through a decoding step 416. At that time, the ciphering part 412 receives a ciphering key 418 from the system of the user. The ciphering part 412 uses the ciphering key 418 and converts the document into a version where the ciphered content 420 is made to be the content. The ciphered content 420 is transferred to an interpretation-use application 424 in a protection shell 422.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－137649
（P2000－137649A）
(43)公開日　平成12年５月16日(2000.5.16)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ｚ	

審査請求　未請求　請求項の数３　ＯＬ　（全 12 頁）

(21)出願番号　特願平11－292595

(22)出願日　平成11年10月14日(1999.10.14)

(31)優先権主張番号　０９／１７８５２９

(32)優先日　平成10年10月23日(1998.10.23)

(33)優先権主張国　米国（ＵＳ）

(71)出願人　590000798
ゼロックス　コーポレイション
ＸＥＲＯＸ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国　06904－1600　コネティカット州・スタンフォード・ロング　リッチ　ロード・800

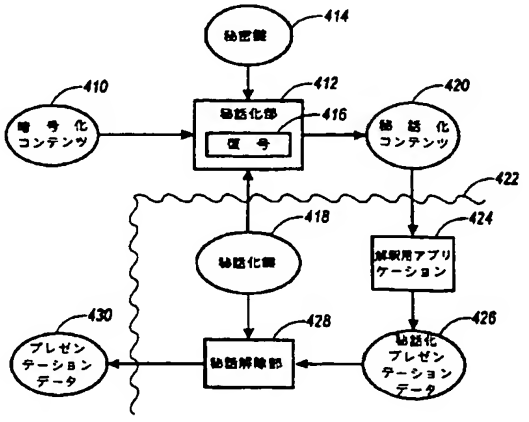
(72)発明者　プラサド　ラム
アメリカ合衆国　カリフォルニア州　マンハッタン　ビーチ　ハーリー　ウェイ　204

(74)代理人　100075258
弁理士　吉田　研二　（外２名）

最終頁に続く

(54)【発明の名称】　自己保護文書システム

(57)【要約】
【課題】　復号処理及び解釈処理時に、不正使用可能な形式の電子配布文書の入手を困難にする。
【解決手段】　電子文書を安全に配布するシステムと方法は、許可受信者であっても未許可受信者であっても、電子文書を無許可で再生・再配布しにくくする。自己保護文書（ＳＰＤ）には、暗号化された文書及びその文書を処理するために必要な許可とソフトウェアで構成されるセキュアセットとが含まれている。文書の完全な復号は、文書が完全に画面上または用紙上に解釈、再生される前に文書の中途取得の可能性を最小限に抑えるために、なるべく遅らせて実行するようにする。



1

【特許請求の範囲】

【請求項１】　文書コンテンツを表すデータが含まれた暗号化コンテンツセグメントと、
許可セグメントと、
コードセグメントと、を含むデータを持った自己保護文書を格納したことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項２】　自己保護文書を作成する方法であって、
未暗号化文書を受け取るステップと、
未暗号化文書を修正してオリジナルコンテンツセグメントを作成するステップと、
権利指定を作成するステップと、
コードセグメントを作成するステップと、
前記オリジナルコンテンツセグメントと前記権利指定と前記コードセグメントを組み合わせて汎用の自己保護文書を作成するステップと、を含むことを特徴とする自己保護文書の作成方法。

【請求項３】　暗号化されたコンテンツセグメントをユーザシステムに持つ自己保護文書を使用する方法であって、
秘話化鍵を取得するステップと、
暗号化コンテンツセグメントを秘話化鍵により修正して秘話コンテンツを作成するステップと、
出力装置に出力できるように秘話コンテンツを解釈し、秘話化解釈コンテンツを作成するステップと、
秘話化鍵を使用して、前記秘話化解釈コンテンツを秘話解除し、平文解釈コンテンツを作成するステップと、
平文解釈コンテンツを出力装置へ送信するステップと、
を含むことを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、文書に対する権利の管理に係り、特に、文書保護のための付加的なソフトウェアまたはハードウェアのサポートを受けずに電子文書の保護を可能にする自己保護文書方式に関する。

【０００２】

【従来の技術】電子商取引を介して電子文書が広範囲に普及するのを妨げている重要な問題の１つは、現段階では、これらの電子文書の配布及び使用時にコンテンツ所有者の知的所有権の保護が十分でない点である。この問題を解決する試みは、「知的所有権管理」（ＩＰＲＭ）、「デジタル所有権管理」（ＤＰＲＭ）、「知的所有管理」（ＩＰＭ）、「権利管理」（ＲＭ）、及び「電子版権管理」（ＥＣＭ）等と呼ばれている。

【０００３】ここで言う文書とは配布または譲渡等が行われる、あらゆる単位の情報のことで、通信文書、書籍、雑誌、ジャーナル、新聞、他の書類、ソフトウェア、写真及び他の画像、オーディオ及びビデオクリップ、その他のマルチメディアプレゼンテーション等であるが、これらに限られているわけではない。文書の具体

2

的な形式は、紙に印刷するか、記憶媒体上の電子データか、または各種媒体上に他の既存の形式で記録されたものである。

【０００４】印刷された文書の場合、著者が作成した著作物は通常は出版業者に渡され、そこで著作物の形式が整えられ大量のコピーが印刷される。これらのコピーは、配送業者により書店または他の小売店に送られ、エンドユーザが購入する。

【０００５】印刷文書の場合、通常はコピーの品質が悪く配布費用も高価であったため、違法コピーは抑止されていた。これに対し、電子文書の場合は保護されていないとコピー、修正、及び再配布がきわめて容易である。したがって、電子文書を保護するための何等かの方法を採用し、違法コピーを簡単に行えないようにする必要がある。このような方法が確立すれば、印刷文書のハードコピーを作成して従来の方法で複写する等は可能であっても、コピーの抑止には役立つと思われる。

【０００６】印刷文書の場合、文書をデジタル化するというステップを踏まないと、電子的に再配布することはできない。この制限は抑止として役立つ。しかし、一般的には、ローカルエリアネットワーク（ＬＡＮ）、イントラネット、及びインターネットを介して接続したパーソナルコンピュータ、ワークステーション、他の装置等の現在の汎用コンピューティング及び通信システムの下では、電子文書を許可を受けずに配布することを防止する有効な方法がないことも現実である。無許可コピーを防止するためにハードウェアを使用して解決する方法も何度か試みられたが、成功したとは言えない。

【０００７】権利の管理には、認証、許可、会計、支払いと金銭上の決済、権利の主張、権利の検証、権利の行使、及び文書の保護等様々な問題がある。この中でも、文書の保護は重要な問題である。ユーザがコンテンツ所有者の権利を認めて文書に対し特別な操作を行うことが許されている場合（印刷したり、画面に表示したり、音楽を演奏したり、ソフトウェアを実行する等）、文書は通常は平文である。つまり、暗号化されていない。簡単に説明すると、文書保護の問題は、文書がもっとも危険な状態（ユーザの管理下にあるマシン上で平文で記憶されている）のときにコンテンツ所有者の権利が侵されないようにすることである。文書が配送業者からユーザに安全に配布された（通常は暗号化された形式）場合でも、その文書を表示データ形式にしないと、ユーザは文書を表示したり操作したりすることはできない。したがって、十分な保護を実現するためには、最終的な段階でユーザに表示され、しかも使用可能な形式に戻しにくい形式で、文書のコンテンツを保護することが重要である。

【０００８】暗号化を使用する電子文書配布の既知の方法では、次のようないくつかのステップを経て処理される。まず、ユーザは暗号化文書を受け取る。次に、ユー

ザは自分の秘密鍵（公開鍵暗号化システム）を使用してデータを復号し、文書の平文の内容を取り出す。最後に、平文の内容は解釈用アプリケーションに渡され、そのアプリケーションがコンピュータ可読文書を最終的な文書に変換し、ユーザのコンピュータ画面で表示したりハードコピーに印刷したりできるようにする。平文のコンテンツを解釈しなければならない理由は、解釈用アプリケーションは通常、サードパーティプロダクト（Microsoft社のWord（商標）やAdobe社のAcrobat Reader（商標）等）であり、入力される文書の形式がそのプロダクトに特有の形式であるからである。

【０００９】

【発明が解決しようとする課題】しかしながら、上記従来の文書の保護方法では、データを平文に復号化する第２のステップとコンテンツを解釈する第３のステップとの間で、それ以前は保護されていた文書であっても危険な状態に置かれる。つまり、復号されていて、しかも、ユーザのコンピュータ上に平文の電子形式で記憶されたままになっているからである。従って、ユーザが不注意だったりまたは経費を節約しようとする場合など、文書はコンテンツ所有者の許可を得ずに容易に再配布されてしまう可能性があるという問題点があった。

【００１０】本発明は、上記実情に鑑みて為されたもので、既知のシステムの欠点を解消し、コンテンツ所有者の許可を得ない再配布を抑止しつつ、電子文書を配布するシステムを提供することを目的とする。このようなシステムが提供されれば、ユーザは復号処理及び解釈処理時に、電子配布文書を再配布可能な形式で入手できなくなる。

【００１１】

【課題を解決するための手段】本発明の自己保護文書（ＳＰＤ）は、上記の従来技術の欠点に対処できる。本発明の記憶媒体に格納された自己保護文書は、暗号化文書と許可セット及びその暗号化文書を抽出して使用するために必要なソフトウェアの大部分が組み込まれた実行可能なコードセグメントとを組み合わせることで、特別なハードウェア及びソフトウェアを使用しなくても文書のコンテンツを保護できる。

【００１２】ＳＰＤシステムは、コンテンツ作成者（従来のモデルの著者及び出版社と類似したもの）とコンテンツ配布業者とに分けられる。著者／出版社はオリジナル文書を作成し、許可する権利を決定する。次に、配布業者が文書をカスタマイズして様々なユーザが使用できるようにするが、その過程で、ユーザの購入した許可範囲をユーザ自身が逸脱しないようにカスタマイズする。

【００１３】ユーザのシステムでは、自己保護文書は最後の段階で復号される。本発明の１実施形態では、ＳＰＤ自身に各種解釈機能も備わっている。そのため、このＳＰＤを使用すれば、信頼度が低い（また許可を受けずに使用することにもなる）外部アプリケーションに頼らなくても済む。別の実施形態では、サードパーティの解釈用アプリケーションのインターフェースとプロトコルを指定し、ＳＰＤと対話的に処理して解釈の信頼度を高めるようにしている。

【００１４】本発明の１実施形態では、暗号化文書はユーザシステムにより復号されるが、同時に、その文書はユーザシステムの状態に少なくとも一部依存している鍵により「秘話化（polarizing）」される。この秘話化は暗号の面からは配布に使用される暗号化処理に比べ安全度は低いが、偶発的なコピーの抑止には役立つ。本発明では、解釈の処理時及びそれ以降に秘話解除が行われ、その結果、文書の中間形式は実質上使用不能になる。

【００１５】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら説明する。

【００１６】図１は、文書の電子配布のシステムの最上位機能モデルを表している。上記で定義したように、これらの文書には、通信文書、書籍、雑誌、ジャーナル、新聞、他の書類、ソフトウェア、オーディオ及びビデオクリップ、及び他のマルチメディアプレゼンテーションが含まれる。

【００１７】著者（または出版社）１１０は文書のオリジナルコンテンツ１１２を作成し、配布業者１１４に渡して配布する。著者が他人を配布業者として使用せずに文書を直接配布することも考えられるが、図１に示したように作業を分割すると効率は向上する。それは、著者／出版社１１０が、配布業者１１４が行う機械的で平凡な役割ではなく、コンテンツの作成に集中できるからである。さらに、このように作業を分担することで、配布業者１１４も多数の著者及び出版社（図示されている著者／出版社１１０も含め）と連携することで、規模の節約を実現できるからである。

【００１８】次に、配布業者１１４は、変換されたコンテンツ１１６をユーザ１１８へ渡す。標準的な電子配布モデルでは、変換されたコンテンツ１１６はオリジナルコンテンツ１１２の暗号化版を表している。つまり、配布業者１１４はユーザ１１８の公開鍵を使用してオリジナルコンテンツ１１２を暗号化し、変換されたコンテンツ１１６は特定のユーザ１１８のためにだけカスタマイズされる。次に、ユーザ１１８は自分自身の秘密鍵を使用して変換されたコンテンツ１１６を復号すれば、オリジナルコンテンツ１１２を表示できる。

【００１９】コンテンツ１１２に対する支払い１２０は、ユーザ１１８から配布業者１１４へ決済機関１２２を介して渡される。決済機関１２２は、ユーザ１１８から、及び特定の文書の表示を希望する他のユーザから要求を収集する。決済機関１２２は、支払い取引、クレジットカード取引、及び他の既知の電子支払い方式等の支払い情報も収集し、収集したユーザの支払いを配布業者１１４へ支払いバッチ１２４として送信する。もちろ

ん、決済機関１２２はユーザの支払い１２０の分け前の一部を受け取る。また配布業者１１４も、支払いバッチ１２４の一部を受け取った上で、著者と出版社１１０へ支払い１２６（印税も含む）を送信する。この方式の１実施形態では、配布業者１１４は特定の１文書に関するユーザ要求をまとめてから送信する。このようにすると、変換されたコンテンツ１１６が含まれた１文書を、すべての要求ユーザが復号できるように生成できる。この生成方法は、本分野では既知である。

【００２０】また、ユーザ１１８が文書を要求（または使用）するたびに、会計メッセージ１２８を監査サーバ１３０へ送る。監査サーバ１３０は、ユーザ１１８の各要求が配布業者１１４が送信する文書と一致することを確認する。そのために、監査サーバ１３０は、会計情報１３１を配布業者１１４から直接受け取る。矛盾が生じたら、その矛盾を報告書１３２を介して決済機関１２２へ送る。これにより決済機関では配布業者１１４へ送る支払いバッチ１２４を調整できる。このような会計方式が確立されているため、この電子文書配布モデルでは詐欺行為が行われる確率が低く、また、使用時間または使用度に応じて料金が変わる時間依存型の使用許可を扱うこともできる。

【００２１】図１に示した上記の文書の電子商取引は、現在一般的に使用されているものである。以下で詳細に説明するように、このモデルは自己保護文書の配布用に説明するシステム及び方法にも同様に適用される。

【００２２】図２には、電子文書配布に関する従来技術のシステムでユーザ１１８（図１）が実行するステップが示されている。上記で説明したように、通常は暗号化装置を使用して文書を暗号化する。次に、暗号化されたこれらの文書を公に配布及び保管し、許可されたユーザが私的に復号する。この形式は、文書の配布業者から目的ユーザまで公衆ネットワークを介して文書を配送したり、安全でない媒体上に文書を記憶したりするときの保護の基本形式である。

【００２３】最初に、ユーザ１１８が暗号化文書２１０を受け取り、復号ステップ２１２へ移る。この分野では既知のように、復号ステップ２１２ではユーザ１１８の秘密鍵を受け取る。この鍵は、ユーザのコンピュータにローカルに記憶しておくか、または必要に応じユーザが入力する。文書２１０を復号すると、オリジナルコンテンツ１１２（図１）と類似または一致する平文コンテンツ２１６が生成される。

【００２４】平文コンテンツ２１６が解釈用アプリケーション２１８へ渡されると、このアプリケーションはプレゼンテーションデータ２２０（つまり、文書のオリジナルコンテンツ１１２の使用可能版）を作成する。通常、このようなシステムでは、プレゼンテーションデータ２２０は文書タイプに従って、ただちにビデオ画面に表示したり、ハードコピーとして印刷したり、または他の目的で使用したりできる。

【００２５】上記で説明したように、このようなシステムでは文書に弱点がある。平文コンテンツ２１６は、配布業者１１４または著者／出版社１１０の承諾または同意なしに、コピー、記憶、または他のユーザへの譲渡が可能である。また、正当なユーザでも、コンテンツ所有者の所有権に配慮せず、文書を平文の形式で受け取って自由に再配布及び使用することでライセンス料の節約を図ろうとするユーザがいる。既に説明したように、本発明では、ユーザシステムでの解釈の処理時に、ユーザが文書を再配布可能な形式で入手できない方式を提供している。

【００２６】したがって、本発明のシステム及び方法では、ユーザ１１８のシステムにおいて暗号化文書を処理する別の方式を提供している。この方式の簡単な実施例を図３に示す。

【００２７】図３は、暗号化文書３１０が復号ステップ３１２（秘密鍵３１４を使用する）及び解釈用アプリケーション３１６へ渡され最終的にプレゼンテーションデータ３１８が作成されるという点において、図２と似ている。しかし、保護シェル３２０により、保護層が別個に用意されている。保護シェル３２０が提供されているため、平文コンテンツを取り込み可能（インターセプト可能）な状態にせずに（図２の平文コンテンツ２１６のように）、文書３１０を復号及び解釈できる。これは、以下に図５を参照して説明するように、文書３１０に復号要素及び解釈要素を組み込むことで実現する。組み込む復号及び解釈要素はユーザのＳＰＤとの対話を制限するように調整され、ユーザ許可に応じて特定の操作（文書の保存またはカットアンドペースト操作の実行）等を制限する。

【００２８】図４はさらに高度なバージョンである。図４の方式には中間「秘話化」（polarizing）ステップ、すなわち、簡易暗号化のステップが含まれていて、復号後で解釈前の文書の安全を確保するように改良されている。まず、暗号化された文書コンテンツ４１０は秘話化部４１２へ渡される。秘話化部４１２はユーザの秘密鍵４１４を受け取り、復号ステップ４１６を介して、文書コンテンツ４１０を復号する。同時に、秘話化部４１２はユーザのシステムから秘話化鍵４１８を受け取る。

【００２９】秘話化部４１２は、この秘話化鍵４１８を使用し、文書を秘話コンテンツ４２０を内容とするバージョンへ変換する。これらの操作はすべて、秘話化部４１２が文書の復号と秘話化処理との間で文書の平文バージョンを記憶していない限り、保護機構を使用せずにオープンで行うことができる。

【００３０】本発明の１実施形態では、秘話化鍵４１８はユーザシステムの内部状態から取り出したデータ要素を組み合わせたものを表している。これらのデータ要素には、日付と時刻、最後のキーストロークからの経過時

間、プロセッサの速度とシリアル番号、及びユーザシステムから継続的に取り出すことができる他の情報等が含まれる。秘話化鍵４１８には、秘話化コンテンツ４２０を取り込んだり獲得したりしてもそのコンテンツが役立たなくなるような時間関連情報を組み込んでおくと便利である。このようにしておけば、システム時間は大幅に変わるため、意味付け文書の解釈は不可能になる。

【００３１】次に、再び保護シェル４２２内で、秘話化されたコンテンツ４２０は解釈用アプリケーション４２４へ渡される。上記で説明したように、標準的な解釈用アプリケーションとしては、Microsoft社のWord（商標）またはAdobe社のAcrobat Reader（商標）等のサードパーティ・アプリケーションである。しかし、このような外部の解釈用アプリケーションは、秘話化されたコンテンツ４２０を処理できない場合も考えられる。これは、コンテンツ、フォーマットコード、及び解釈処理側で使用する指示符号が秘話化処理時にスクランブルされるからである。

【００３２】したがって、解釈用アプリケーション４２４には互換性（又は少なくともフォルト・トレラント性）が要求され、若しくは、ほぼ完全でアプリケーションが処理可能な秘話化コンテンツ４２０を受け取らなければならない。後者の可能性については、図９と共に以下に説明する。

【００３３】解釈用アプリケーションの出力は秘話化プレゼンテーションデータ４２６（秘話化解釈コンテンツ）で、これは解釈用アプリケーション４２４によりフォーマットされているが、まだ秘話化されたままであるため、ユーザがそのまま読み取ることはできない。秘話化プレゼンテーションデータ４２６は秘話解除部４２８に渡され、その秘話解除部が秘話化鍵４１８を受け取って文書の元の形式をプレゼンテーションデータ４３０（平文解釈コンテンツ）として復元する。本発明の１実施形態では、この秘話解除機能は解釈の機能または表示機能と組み合わされている。この場合、秘話化プレゼンテーションデータ４２６は表示装置が直接受け取る。この表示装置はユーザシステムと別個のもので、通信チャネルを介してデータを受け取るものであっても構わない。

【００３４】秘話化鍵４１８の作成、解釈用アプリケーション４２４、及び秘話解除ステップ４２８は、すべて保護シェル４２２の構成要素である。これらは変更が困難なプログラム要素である。保護シェル４２２の内部で実行されるすべての計算ステップはローカルデータだけを使用し、グローバルにアクセス可能な記憶媒体やメモリー領域へは一時データを格納しない。最終的に明示できる結果だけを保護シェル４２２からエクスポートする。この方法により、中間データを中途で盗用したり、利用したりする目的で、ユーザが簡便な手法をとることができなくなる。例えばオペレーティングシステムのエントリー・ポイントを修正したり、システム資源を窃取したりすることができなくなる。

【００３５】本発明の別の実施の形態では、図４のプレゼンテーションデータ４３０はデバイス非依存型データまたはデバイス依存型データのいずれでも構わない。デバイス非依存型の場合、解釈処理を完了するためには、通常、デバイスドライバ（表示ドライバまたはプリンタドライバ等）による追加処理が必要になる。現時点での好ましいデバイス非依存型データの場合、プレゼンテーションデータに対する各デバイスへの適合補正は（解釈用アプリケーション４２４または秘話解除ステップ４２８のいずれかで）すでに行われていて、プレゼンテーションデータ４３０を目的の出力装置に直接出力できる。

【００３６】図３及び図４を使用して説明した上記の復号方式は、図５で詳細に示している独自の文書のデータ構造により実現される。上記で説明したように、本発明のシステム及び方法が実行する特定の操作では、高信頼性の構成要素が必要である。特定の純正コード（修正されていないコード）を使用して本発明の信頼性を向上させる方法の１つは、このコードを文書と共に提供することである。かかる方法を具現化する本発明による自己保護文書の各種データ構成要素については、図５で説明する。

【００３７】本発明による文書保護の問題解決方法は、ユーザシステム側で高信頼性ハードウェア装置またはソフトウェアモジュールを用意していないという前提で使用される。これを実現するために、文書の機能を強化し、アクティブなメタ文書オブジェクトにする。コンテンツ所有者（つまり著者または出版社）は、文書に権利情報を付加し、使用目的のタイプ、必要な許可と関連料金、及びユーザに許可を与えるソフトウェアモジュールを指定する。文書と、関連する権利と、権利の行使を実現する付加ソフトウェアモジュールを組み合わせたものが、本発明にいう自己保護文書（ＳＰＤ）である。自己保護文書では許可されていなかったり、想定されていない管理外の使い道や文書の配布が防止されるため、コンテンツ所有者の権利が保護される。

【００３８】自己保護文書５１０は、次の３種類の主要機能セグメントにより構成されている。実行可能コードセグメント５１２には、ユーザが暗号化文書を使用するために必要な実行可能コード部分が含まれている。権利及び許可セグメント５１４には、さまざまなユーザに許可する各種アクセスレベルを表すデータ構造体が含まれている。コンテンツセグメント５１６には、ユーザが表示する暗号化コンテンツ１１６（図１）が含まれている。

【００３９】本発明の好適な実施形態では、ＳＰＤ５１０のコンテンツセグメント５１６は、文書メタ情報５１８（文書のタイトル、フォーマット、及び改訂日等の情報）、権利ラベル情報５２０（テキストと共に表示する

著作権の表示と権利及び許可情報）、及び保護コンテンツ５２２（暗号化された文書自身）の３種類のサブセクションで構成される。

【００４０】本発明の１実施形態では、権利及び許可セグメント５１４には、各許可ユーザごとの権利情報が含まれる。料金及び条件の一覧を、各ユーザの権利に加えても構わない。例えば、John Doeというユーザに特定の文書を表示する権利と、２回だけ印刷する権利とを１０ドルで与えることができる。この場合、権利及び許可セグメント５１４ではJohn Doeを識別し、彼に２種類の権利を関連付け（表示権及び印刷権）、価格（１０ドル）及び印刷の制限（２回）等の料金と条件を指定する。権利及び許可セグメント５１４には、他のユーザの情報を組み込んでも構わない。

【００４１】別の実施形態では、権利及び許可セグメント５１４には権利情報を指定する外部情報へのリンクだけを組み込む。この場合、実際の権利及び許可はネットワークで接続された許可サーバ等の別の場所に記憶されていて、文書を使用するたびに照会を行う必要がある。この方法では、権利及び許可をコンテンツ所有者が動的に更新できるという利点がある。例えば、表示のための価格を引き上げたり、許可されていない態様での使用を検出したらユーザの権利を無効にしたりできる。

【００４２】いずれの場合にも、権利及び許可セグメント５１４は暗号で署名し（本技術分野では既知の方法により実現できる）、指定された権利及び許可を不正に変更できないようにするのが好ましい。また、ユーザが自分自身及び他人の権利及び許可を直接表示できないように暗号化することも好ましい。

【００４３】実行可能コードセグメント５１２（「ＳＰＤ制御」とも呼ばれる）にも幾つかのサブセクションが含まれていて、各サブセクションは、少なくとも一部が実行可能コードセグメントに含まれるソフトウェアで構成されている。本発明の１実施形態では、このＳＰＤ制御にJavaプログラミング言語を使用している。しかし、本発明を実現するには、プラットフォームに依存しない言語であるかプラットフォームに固有の言語（インタプリタ型またはコンパイラ）であるかに関わらず、任意の言語を使用できる。

【００４４】権利行使部５２４は、ユーザのＩＤを確認し、ユーザが要求するアクションと権利及び許可セグメント５１４に列挙されているアクションとを比較し、指定された権利に基づいて要求されたアクションを許可または拒否するために用意されている。権利行使部５２４の処理は、図７を参照して以下に詳細に説明する。

【００４５】秘話化エンジン５２６も、実行可能コードセグメント５１２に、保護された状態で含まれている。このエンジンは、既に説明したように、システムの状態（または他の秘話化鍵）に従ってデータを読み取り、秘話化する。本発明の好適な実施形態では、秘話化エンジン５２６は文書の記憶前または復号前にその文書を処理するため、ユーザシステムに文書が平文で記憶されることはない。秘話化エンジン５２６は保護されていて（つまり、暗号署名及び暗号化されていて）、変更、リバースエンジニアリング、及び逆アセンブルできないようになっている。

【００４６】対応する秘話解除エンジン５２８も実行可能コードセグメント５１２に含まれていて、秘話化コンテンツから平文のプレゼンテーションデータを生成できるようにしている（図４を参照されたい）。秘話解除エンジンにはセキュアウィンドウオブジェクトの組が含まれていて、ユーザシステムの解釈用ＡＰＩ（Application Program Interface）に対する変更防止インターフェースになっている。セキュアウィンドウオブジェクトは途中取り込みが困難である。このため、オペレーティングシステム用のデータを途中取り込み、又は受信して平文形式の文書を再構築する機会を少なくできる。

【００４７】実行可能コードセグメント５１２に含まれている、対応する秘話解除エンジン５２８は、秘話化されたコンテンツから平文のプレゼンテーションデータを生成できる（図４を参照されたい）。また、この秘話解除エンジン５２８は、論理出力装置または物理出力装置（例えば、ユーザの表示装置）に対する変更防止インターフェースである。秘話解除エンジン５２８に入力されるのは、秘話化プレゼンテーションデータである。したがって、そのデータが中途で取り込まれても、ユーザのシステム状態等に依存する秘話解除の処理を実行しないと平文コンテンツは得られない。すなわち、たとえ中途でデータが取り込まれてしまっても、そのデータは各システムに特有の状態情報に基づいて秘話化されているため、平文コンテンツの取得がきわめて困難になっているのである。

【００４８】セキュア表示部５３０は、実行可能コードセグメント５１２にオプションで組み込まれる。セキュア表示部５３０は、権利及び許可セグメント５１４に基づき、許可されているアクセスレベルだけを許可するために使用される。例えば、ユーザが文書を表示する権利しか買っていない場合（保存（セーブ）や印刷の権利は買っていない）には、表示部は、ユーザに対し保存や印刷は許可せず、また、現在の大部分のオペレーティングシステムで実行可能なカットアンドペーストの実行も許可しない。

【００４９】また、解釈用エンジン５３２が実行コードセグメント５１２に含まれているか、または、実行コードセグメント５１２により参照される。解釈用エンジン５３２は、保護する必要はない。したがって、解釈用エンジン５３２のコードはＳＰＤアプレット内に組み込まれていてもよいし、他の場所から（セキュアリンクを介して）取得することとしても構わない。どちらの場合も、解釈用エンジン５３２は、秘話化文書コンテンツの

入力を受けて、当該コンテンツデータから秘話化プレゼンテーションデータを作成するように設定されている（図４を参照されたい）。

【００５０】自己保護文書５１０の上記の態様及び要素を、システムの動作と共に、以下に詳細に説明する。

【００５１】図６は、自己保護文書５１０が作成され、配布されるときに実行されるステップを示したものである。汎用（generic）ＳＰＤ６１０には、ユーザ固有の権利情報は組み込まれておらず、特定のユーザ用に暗号化もされていない。汎用ＳＰＤ６１０は、３つの項目、すなわち、平文（暗号化されていない）形式のオリジナル文書コンテンツ６１２、高レベル権利指定６１４、及びオプションの透かし６１６から作成される。

【００５２】コンテンツ６１２は、著者または出版社の希望に合わせて、文書のレイアウトを決定するように事前処理（プリプロセス）される（ステップ６１８）。例えば、希望するページサイズ、フォント、及びページレイアウトを選択できる。コンテンツ６１２は、ユーザシステム及びＳＰＤと互換性がある形式になるように、コンテンツ事前処理ステップで実際に「事前解釈」される。例えば、コンテンツ６１２はMicrosoft Word（「.DOC」）またはAdobe Acrobat（「.PDF」）形式から解釈用エンジン５３２が読み取れるように特別に設定された別の形式に変換される（図５）。本発明の１実施形態では、コンテンツ６１２の複数のバージョンがコンテンツ事前処理ステップで生成され、汎用ＳＰＤ６１０に記憶される。ユーザは、これらの異なったバージョンを、要求に応じて個別に購入できる。

【００５３】高レベル権利指定６１４では、アクセス権利の可能な組合せを記述する。この権利指定は、文書ごとに合わせて設定され、下流のユーザの様々なクラスの様々な権利グループを記述できる。例えば、１コピー当り１．００ドル、追加コピーに２．００ドルの使用料で最大１００，０００部の文書を配布する権利を出版社に与えることができる。同様に、１ヶ月後や１年後に「期限切れ」する文書または期限のない文書等、各バージョンの文書購入オプションをユーザに与えることができる。考えられるいくつかの制限について、詳細な例を参照して説明する。以下に例を述べる。

【００５４】Digital Property Rights Language（ＤＰＲＬ）は、デジタル著作の権利を指定するために使用される言語である。この言語は、権利に関する各種料金及び条件を指定し、権利を行使する機能を提供している。権利指定は、ＤＰＲＬのステートメントとして表現される。詳細については、Stefikに付与された米国特許第５，７１５，４０３号、「System for Controlling the Distribution and Useof Digital Works Having Attached Usage Rights Where the Usage Rights areDefined by a Usage Rights Grammar」等を参照。権利の行使及び権利に関連する条件の検証は、ＳＰＤ技術を使用て行われる。

【００５５】各種権利は、「ｗｏｒｋ（ワーク）」指定を使用してデジタル著作物の各要素について指定できる。ｗｏｒｋ指定では、各著作に適用可能な各種の権利のセットを指定できる。権利は、「right group」と呼ばれる名前付きグループに分類できる。権利グループ内の各権利は、条件セットに関連付けられる。条件には、支払う料金、使用時間、アクセスタイプ、透かしタイプ、処理を行う装置タイプ等様々な種別がある。ＤＰＲＬでは、譲渡、表現権、派生著作権、ファイル管理権、及び構成権等の各種権利カテゴリに対応している。トランスポート権は、ある格納場所（レポジトリ）から別のレポジトリへの著作物の移動に関する。表現権は、著作物の印刷及び表示、より一般的には、変換装置を介して著作物を外部媒体へ送信することに関する（これには、平文のコピーを作成するために使用する「エクスポート」権も含まれる）。派生著作権は、新しい著作物を作成する場合に著作物の再使用をすることに関する。ファイル管理権は、バックアップコピーの作成及び復元に関する。また、構成権はレポジトリのソフトウェアのインストールをに関する。

【００５６】ＤＰＲＬのワーク指定の例を以下に示す。

【００５７】

```
(Work:
    (Rights-Language-Version: 1.02)
    (Work-ID: "ISDN-1-55860-166-X; AAP-2348957tut")
    (Description: "Title: 'Zuke-Zack, the Moby Dog Story'
        Author: 'John Beagle'
        Copyright 1994 Jones Publishing")
    (Owner: (Certificate:
            (Authority: "Library of Congress")
            (ID: "Murphy Publishers")))
    (Parts: "Photo-Celebshots-Dogs-23487gfj" "Dog-Breeds-Chart-AKC")
    (Comment: "Rights edited by Pete Jones, June 1996.")
    (Contents: (From: 1)(To: 16636))
    (Rights-Group: "Regular"
```

```
(Comment: "This set of rights is used for standard retail editions."
)
(Bundle:
(Time: (Until: 1998/01/01 0:01))
    (Fee: (To: "Jones-PBLSH-18546789")(House: "Visa")))
(Play:
    (Fee (Metered: (Rate: 1.00 USD)(Per: 1:0:0)(By: 0:0:1)) ))
(Print:
    (Fee: (Per-Use: 10.00 USD))
    (Printer:
        (Certificate:
            (Authority: "DPT"
            (Type: "TrustedPrinter-6")))
    (Watermark:
        (Watermark-Str: "Title: 'Zeke Zack - the Moby Dog'
                         Copyright 1994
                         by Zeke Jones.
                         All Right Reserved.")
        (Watermark-Tokens: user-id institution-location
                           render-name render-time) )))
(Transfer:)
(Copy: (Fee: (Per-Use: 10.00 USD) ))
(Copy: (Access:
        (User: (Certificate:
            (Authority: "Murphy Publishers")
            (Type: "Dustributor")))))
(Delete:)
(Backup:)
(Restore:    (Fee: (Per-Use: 5.00 USD))) ))
```

【００５８】このｗｏｒｋ指定には「Regular」と呼ばれる権利グループがある。これは、「Zuke-Zack, the Moby Dog Story」という題名の書籍の標準小売版の権利を指定している。このワーク指定は、表示再生（ｐｌａｙ）、印刷（ｐｒｉｎｔ）、転送（ｔｒａｎｓｆｅｒ）、コピー（ｃｏｐｙ）、削除（ｄｅｌｅｔｅ）、バックアップ（ｂａｃｋｕｐ）、及びリストア（ｒｅｓｔｏｒｅ）等の幾つかの権利の条件を表している。この例の著作物には、他のソースから組み込まれた、さらに２つの構成要素として、写真と犬の種類表（chart of breeds）とが含まれている。「bundle」指定は、グループ内のすべての権利に適用される共通の条件セットをまとめている。この指定は、グループ内のすべての権利が１９９８年の１月１日まで有効で、料金をアカウント「Jones-PBLSH-18546789」に支払うことを表している。この取引の決済機関はＶｉｓａである。さらに以下に述べる契約が適用される。著作物の再生には１時間当り１．００ドル支払い、料金は秒単位で累算される。著作物は「ＤＰＴ」により保証されるTrustedPrinter-6で印刷でき、１回の印刷当り１０．００ドルの料金である。印刷されたコピーには、（上記のように設定された）透かし文字列と印刷時に分かっている「指紋（finger print）」としてのトークンリストとを付ける。この著作物は、１０．００ドル支払うかまたはＭｕｒｐｈｙ出版から配布業者証明書を入手してコピーできる。この著作物の無制限の譲渡、削除、またはバックアップが許されている（リストア・コスト５．００ドル）。

【００５９】高レベル権利指定６１４も事前処理ステップの対象になる（ステップ６２０）。この場合、高レベル（人間が読み取り可能な）指定は、より効果的なデータ構造表現にコンパイルされ、本発明で使用できるような形式になる。

【００６０】次に、事前処理されたコンテンツ６１２、事前処理された権利指定６１４、及び透かし６１６を組み合わせることで汎用ＳＰＤ６１０を作成する（ステップ６２２）。透かしは、本技術分野で知られている任意の方法で付加できる。ＳＰＤにおける透かしは、目で確認できる形式でも、できない形式でもよい。汎用ＳＰＤ６１０は、著者／出版社１１０によりオプションで暗号化し、配布業者１１４へ送信してもよい（図１）。

【００６１】次に、配布業者１１４は汎用ＳＰＤ６１０を受け取り、後でカスタマイズできるように記憶格納す

る。配布業者１１４がユーザ要求６２４を受け取ると（直接、または決済機関１２２あるいは他の中間機関を介して）、配布業者１１４は、ユーザ要求６２４、及び権利指定６１４の両方と互換性のあるユーザ許可のセットを作成する（ステップ６２６）。このような互換性のある許可セットがない場合は、ユーザのためのアクションはこれ以上実行されない（オプションでユーザに対し出される通知メッセージを除く）。

【００６２】次にユーザ許可及びユーザの公開鍵６２８を使用し、ユーザが使用できる形式に設定されたカスタマイズＳＰＤ６３２を生成する（ステップ６３０）。ステップ６２６で入手したユーザ許可をＳＰＤ６３２の権利及び許可セグメント５１４に記憶し、ユーザの公開鍵６２８を使用してＳＰＤ６３２のコンテンツセグメント５１６のコンテンツを暗号化する。ここでは公開鍵暗号化機構を使用して、ＳＰＤを汎用形式からカスタマイズＳＰＤ６３２へ変換できる。この機構は、著者、出版社、小売店、顧客等、様々な関係者間で、各段階で権利を保護しながらＳＰＤの機密を守って受け渡しする場合に便利である。さらに、複数のユーザ要求を１つのＳＰＤ６３２内に作成し、格納できることにも注意する必要がある。この技術としては、複数の公開鍵を使用して文書を暗号化し、しかも、任意のユーザ秘密鍵を使用して復号できるような技術が知られている。

【００６３】その結果得られるカスタムＳＰＤ６３２は、コンピュータネットワーク等の利用可能な手段によりユーザ１１８へ送信するか、または物理媒体（磁気ディスクまたは光ディスク等）に格納して頒布される。

【００６４】ユーザがＳＰＤを受け取ったときに実行する操作を図７のフロー図に示してある。まず、ＳＰＤが受け取られ、ユーザシステムに記憶される（ステップ７１０）。通常は、ＳＰＤをただちに使用する必要はない。使用したいとき、通常はユーザ名とパスワードまたは鍵を用いて、最初にユーザの認証が行われる（ステップ７１２）。次に、システムはユーザが希望するアクションを判別する（ステップ７１４）。アクションが選択されると、本発明の権利行使ステップ（ステップ７１６）が実行され、希望するアクションに関連する条件を検査する（料金、時間、アクセスレベル、透かし、または他の条件等）。これは、実行可能コードであるＳＰＤアプレット５１２（図５）によりローカルに行うか、または権利実施サーバにアクセスすることで実行できる。

【００６５】権利行使ステップ（ステップ７１６）が失敗すると、更新手順（ステップ７１８）が実行される。ここでユーザは、追加料金を承認するなど、自分の許可を更新する機会が与えられる。条件の検査が正常に終了すると、事前監査手順（ステップ７２０）が実行され、ＳＰＤシステムは検査状態をトラッキングサービス（図１の監査サーバ１３０等）へ記録する。これで、コンテンツは既に説明したように確実に解釈され、画面に表示再生される（ステップ７２２）。ユーザの処理が終了すると、事後監査手順（ステップ７２４）が実行され、使用量がトラッキングサービスにより更新される。そして、ＳＰＤシステムは次のアクションを待つ。

【００６６】ＳＰＤによる保護において特徴的なことは、解釈処理時の中間段階では、ユーザが文書を再配布等の不正利用可能な形式では入手できないようにしていることである。これは、できるだけ後段で、できれば最後のステップで文書コンテンツを復号することで実現されている。

【００６７】図８に、ＳＰＤ復号モデルを示す。Ｅは出版社が実行する暗号機能を示し、Ｄはユーザシステムで実行される復号を示し、Ｒは解釈変換処理を示す。従来システムの多くは最初の変換シーケンスである経路８１０、つまり、Ｄ（Ｅ（ｘ））を実行した後、引き続いてＲ（Ｄ（Ｅ（ｘ））を行っている。既に述べたように、初期の段階で行われる復号では文書は危険な状態に置かれる。できれば、変換は逆順である経路８１２、つまりＲ’（Ｅ（ｘ））を実行した後、引き続いてＤ（Ｒ’（Ｅ（ｘ））を実行するとよい。これにより、復号は可能な限り後段で行われる。

【００６８】Ｒ’が可能かどうか、つまり、復号の前に解釈の処理を実行できるかどうかは、以下の式により判別する。

【００６９】

Ｄ（Ｒ’（Ｅ（ｘ））＝Ｒ（Ｄ（Ｅ（ｘ））

ここで、暗号化関数と復号関数とが可換である場合、つまり、任意のｘに対してＥ（Ｄ（ｘ））＝Ｄ（Ｅ（ｘ））となる場合には、Ｒ’が可能かどうかは次の式で確認できる。

【００７０】

ｙ＝Ｅ（ｘ）についてＲ’（ｙ）＝Ｅ（Ｒ（Ｄ（ｙ））

実際には、ＲＳＡシステム及びＥＩＧａｍａｌ離散対数システム等の一般的な公開鍵暗号システムの暗号化及び復号関数はこの可換性の要求を満足する。つまり、暗号化及び復号にこれらの復号システムを使用する場合、変換Ｒ’は可能である。

【００７１】パスｘ’＝Ｄ（Ｒ’（Ｅ（ｘ））は、許可されない文書の使用及び配布に対する文書保護の理想的なＳＰＤによる解決方法を示している。文書の配布及び使用のシナリオを以下に説明する。ユーザが文書を購入すると、文書はユーザの公開鍵情報を使用して暗号化し、インターネット等の安全でないネットワークチャネルを介して送信する。暗号化した文書には権利情報が追加されており、権利及び許可を実行する保護アプレット５１２がコンテンツ所有者によりユーザに付与されている。ユーザが文書の使用を要求すると、このアプレットは権利及び許可を確認し、オリジナル文書のプレゼンテーション形式を暗号化文書から生成する。最終的なプレ

ゼンテーションデータ形式になる前の文書の中間形式はどの形式でもユーザの秘密情報により暗号化されているため、文書保護のＳＰＤモデルでは、この文書の中間形式が途中取り込みされても他のシステムでは使用できないことが保証されている。

【００７２】この理想的なモデルは、解釈変換処理Ｒに対応する変換処理Ｒ'の計算が効果的に行えるかどうか、特に、Ｒ'実行時に復号関数Ｄを呼び出すことが必要かどうか、に依存していることは明らかである。Ｒ'を効果的に実行できる場合で問題にしなくてもよい自明なケースは、Ｒが暗号化関数Ｅと可換である場合である。この場合、ｙ＝Ｅ（ｘ）について

Ｒ'（ｙ）＝Ｅ（Ｒ（Ｄ（ｙ））＝Ｒ（Ｅ（Ｄ（ｙ））＝Ｒ（ｙ）

となる。尚、この場合、Ｒ'＝Ｒである。

【００７３】図８から分かることは、２つの極端なケースｘ'＝Ｒ（Ｄ（Ｅ（ｘ））、つまりｘ＝Ｄ（Ｅ（ｘ））に対し保護がない場合とｘ'＝Ｄ（Ｒ'（Ｅ（ｘ））（理想的な保護）との間には、文書保護の問題に対するいくつかの中間的な解決方法（例えば、中間解決方法８１４、８１６、及び８１８）が存在する（上記の想定の下で）ということである。図８に示してあるように、暗号化された文書Ｅ（ｘ）からプレゼンテーションデータｘ'を得るには様々なパスがあり、それらは、部分的な解釈変換処理と部分的な復号変換処理が様々に組み合わされたデータに対応していることが分かる。この場合も、どのパスでも復号Ｄを遅らせることで文書の保護レベルが向上することがわかる。

【００７４】上述のように、復号処理をできるだけ遅らせるという代替的方法では、文書全体や形式ではなく文書のコンテンツだけを暗号化する秘話化技術を採用している。この実現方法を図９に示す。文書コンテンツ９１０は最初は平文である（これは、ユーザ処理時に認識可能な単一の箇所でではなく、図４のステップ４１２実行時に発生する一時的な状態である）。文書は、データ部分９１４と形式部分９１６とに分割される（ステップ９１２）。データ部分９１４は秘話化鍵９２０を使用して秘話化され（ステップ９１８）、平文形式部分９１６とマージされる（ステップ９２２）。これにより、秘話化コンテンツ９２４が得られる。この秘話化コンテンツは、コンテンツを復号しなくても秘話化プレゼンテーションデータに解釈可能である。この秘話化形式の安全性は、秘話化鍵による本格的な暗号化よりも低い。なぜなら、文書のレイアウト、ワードの長さ、行の長さ等から大量の情報が得られ、従って概略の内容が判明してしまうからである。しかし、この方式は、偶発的な著作権侵害を抑止できる。

【図面の簡単な説明】

【図１】　安全な環境または安全でない環境における電子文書の作成及び商用配布のモデルを表す最上位レベルブロック図である。

【図２】　従来技術による保護電子文書の復号を表すフローチャート図である。

【図３】　本発明の簡単な実施形態による保護電子文書の復号を表すフローチャート図である。

【図４】　本発明の好適な実施形態による保護電子文書の復号を表すフローチャート図である。

【図５】　本発明の１実施形態による自己保護文書のデータ構造を表す機能ブロック図である。

【図６】　本発明の１実施形態による自己保護文書の作成及びカスタマイズを表すフローチャート図である。

【図７】　ユーザの立場から見た、本実施形態による自己保護文書の処理及び使用時に実行される処置を表すフローチャート図である。

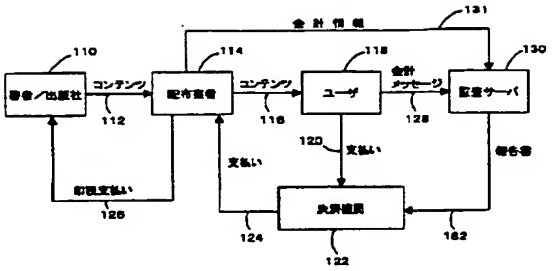
【図８】　未解釈・暗号化文書と解釈済み・復号化プレゼンテーションデータ間の考えられるパスを表すグラフである。

【図９】　文書形式情報を解釈用に平文の状態にした、本発明による秘話化処理を表すフローチャート図である。

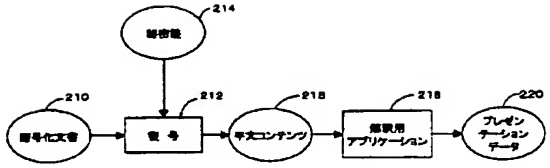
【符号の説明】

３１０　暗号化文書、３１４　秘密鍵、３１６　解釈用アプリケーション、３１８　プレゼンテーションデータ、４１０　暗号化コンテンツ、４１２　秘話化部、４１４　秘密鍵、４１８　秘話化鍵、４２０　秘話化コンテンツ、４２４解釈用アプリケーション、４２６　秘話化プレゼンテーションデータ、４２８秘話解除部、４３０　プレゼンテーションデータ、５１２　実行可能コード、５１４　権利および許可、５１６　コンテンツ、５１８　文書メタ情報、５２０権利ラベル情報、５２２　保護コンテンツ、５２４　権利行使部、５２６　秘話化エンジン、５２８　秘話解除エンジン、５３０　セキュア表示部、５３２　解釈用エンジン、６１０　汎用ＳＰＤ、６１２　コンテンツ、６１４　権利指定、６１６　透かし。

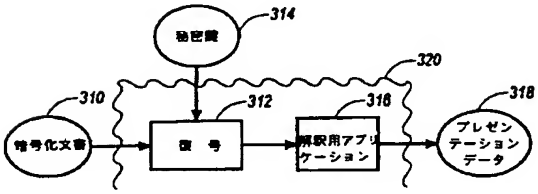
【図１】



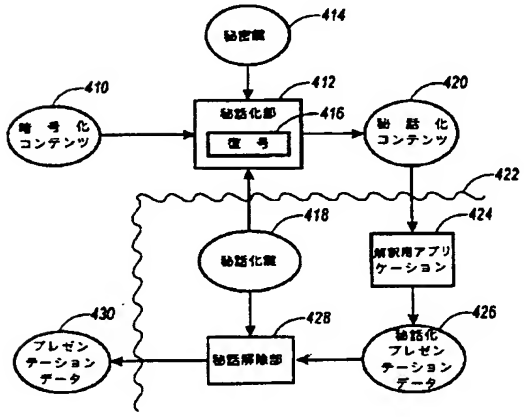
【図２】



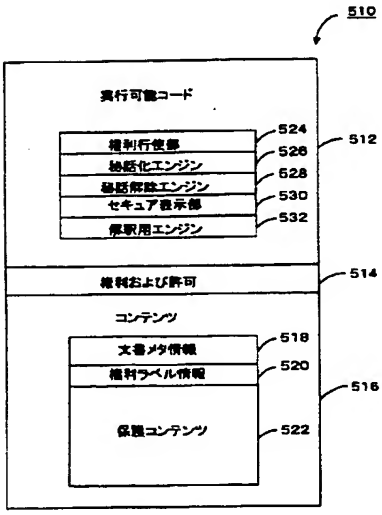
【図３】



【図４】



【図５】



【図６】